ARMS i Snort Central

CARNetovi sigurnosni servisi

Ivor Milošević @srce.hr

I Dio: ARMS

AIDE Repository Management Suite

AIDE

Instalacija i konfiguracija

Korištenje

Početak:

- Tripwire:
  - IDS?
  - Provjera integriteta datoteka
- Potreba za nadgledanjem ključnih ili nepromjenjivih atributa datoteka:
  - Veličina binarnih potpisa
  - Očekivana promjena veličine (npr. logovi)
  - Permissions, md5/sha1 checksum, user, group, itd...

Što je AIDE?

- **AIDE** je besplatni klon Tripwirea
  - Tripwire je postao komercijalan
- Generira i uspoređuje karakteristične "potpise" datoteka
- Potpisi prikupljeni u trenutku kada je sustav u ispravnom stanju spremaju se u bazu
- Nalaženjem kasnije nastalih razlika otkrivaju se izmjene na sustavu

Problem:

- “Potpise” treba spremati na medij koji ne dozvoljava izmjene, brisanje

- Scenarij:
  - Računalo je provaljeno
  - Provalnik instalira trojanske alate
  - Napravi novu aide bazu, ukloni staru
  - Tragovi su skriveni

Rješenja:

- Bazu zapržiti na CD
  - Vrijedi do slijedeće dogradnje
  - Jeftin medij
  - Nije prijateljski odnos prema okolišu
- Snimati na medij koji se može “zaključati”
  - Disketa
  - ZIP disk
  - Vanjski USB/Firewire disk
  - ...

Ili, elegantnije...

- Bazu potpisa držati na sigurnom mrežnom poslužitelju
  - Čuvaju se i starije baze, moguće je pratiti razvoj situacije
  - Jednostavnost i lakoća rada
  - Web sučelje

ARMS

- Kao odgovor na taj zahtjev razvijen je:

  AIDE Repository Management Suite

- Sastoji se od:
  - Poslužitelja `aidexfd`
  - Klijenta `aidexfer`

Realizacija

- razvijen u Perl-u
- koristi MySQL bazu za nadzor i upravljanje serverom
- web-server kao sučelje za pristup podacima
- komunikacija klijenta i servera odvija se kriptografski zaštićenim kanalom (SSL)

ARMS

Instalacija i konfiguracija

Instalacija klijenta:

- Naredba:

 # apt-get install aide-arms-client

- Instalirat će sve potrebne dodatne pakete:
  - Aide, perl, debconf, libnet-ssleay-perl, libconfig-general-perl, libterm-readkey-perl

Slijedeći korak je editiranje spisa **/etc/aide/aidexfer.conf**.

```
# /etc/aide/aidexfer.conf
# client configuration
# uncomment to enable server certificate verification
CA_file /usr/local/aidexfer/lib/localca.crt
# connection address
Server phobos.carnet.hr:2121
# authentication tokens
Username: LDAP_USERNAME
Password:  LDAP_PASSWORD
# storage identification (overrideable)
ProStor IME_ZA_STORAGE
```

AIDE konfiguracija

- /etc/aide/aide.conf

```
# Custom rules
ImePravila = p+i+n+u+g+s+b+m+c+md5+sha1

# Next decide what directories/files you want in the
    database

# Moja Pravila
/direktorij ImePravila
```

AIDE konfiguracija

- /etc/default/aide
- MAILTO=root
- #QUIETREPORTS=1
- COMMAND=update
- LINES=1000
- …

- /etc/cron.daily/aide

ARMS

Korištenje

aidexfer

- Većina parametara zadaje se komandnom linijom
- Pomoć:

```
# aidexfer  --help
```

usage: aidexfer [options] command arg

- opcije:

```
-f | --config <config_file>
-s | --server
<server>:<port>
-r | --prostor <protected-
storage>
-u | --username <username>
-p | --password <password>
-o | --outfile <filename>
-I | --hi-security
-w | --writeconf
-v | --verbose
-g | --debug
-h | --help
```

- naredbe:

```
init -- initialize protected
storage
list -- lists protected storage
wide-list -- listing with more
details
store-db -- stores <arg.db> file
retrieve-db -- retrieves <arg.db>
file
store-cf -- stores config file
retrieve-cf -- retrieves config
file
test -- just test authorization
new-user -- create read-only user-
account
set-passwd -- set password for the
latter
new-prostor -- allocate protected
storage
```

Primjer korištenja:

- Kreiranje spremišta:

 # aidexfer --prostor test_12 init

- Testiranje autentikacije i mogućnosti pristupa nekom spremištu:

 # aidexfer --prostor test_12 test

- Pohrana aide.db baze u defaultno spremište:

 # aidexfer -l store-db aide.db

- Dohvat posljednje pohranjene baze:

 # aidexfer --outfile aide-latest.db retrieve-db latest

- Detaljni ispis sadržaja spremišta:

 # aidexfer wide-list

Provjera:

- Primjer:

 # aidexfer -o /var/lib/aide/aide.db retrieve-db latest

Skida najnoviju AIDE bazu sa ARMS repozitorija na lokalni disk, u /var/lib/aide/aide.db.

- Moguća je potpuna automatizacija dijagostike integriteta datoteka.

Provjera:

- AIDE za provjeru integriteta datotečnog sustava koristi bazu /var/lib/aide/aide.db

- Pokretanje AIDE provjere:

  # aide --check

Nakon provjere:

- Slanje nove baze na centralni server:

  aidexfer store-db /var/lib/aide/aide.db.new

- **Osvježavanje baze:**

  # cd /var/lib/aide
  # mv aide.db.new aide.db

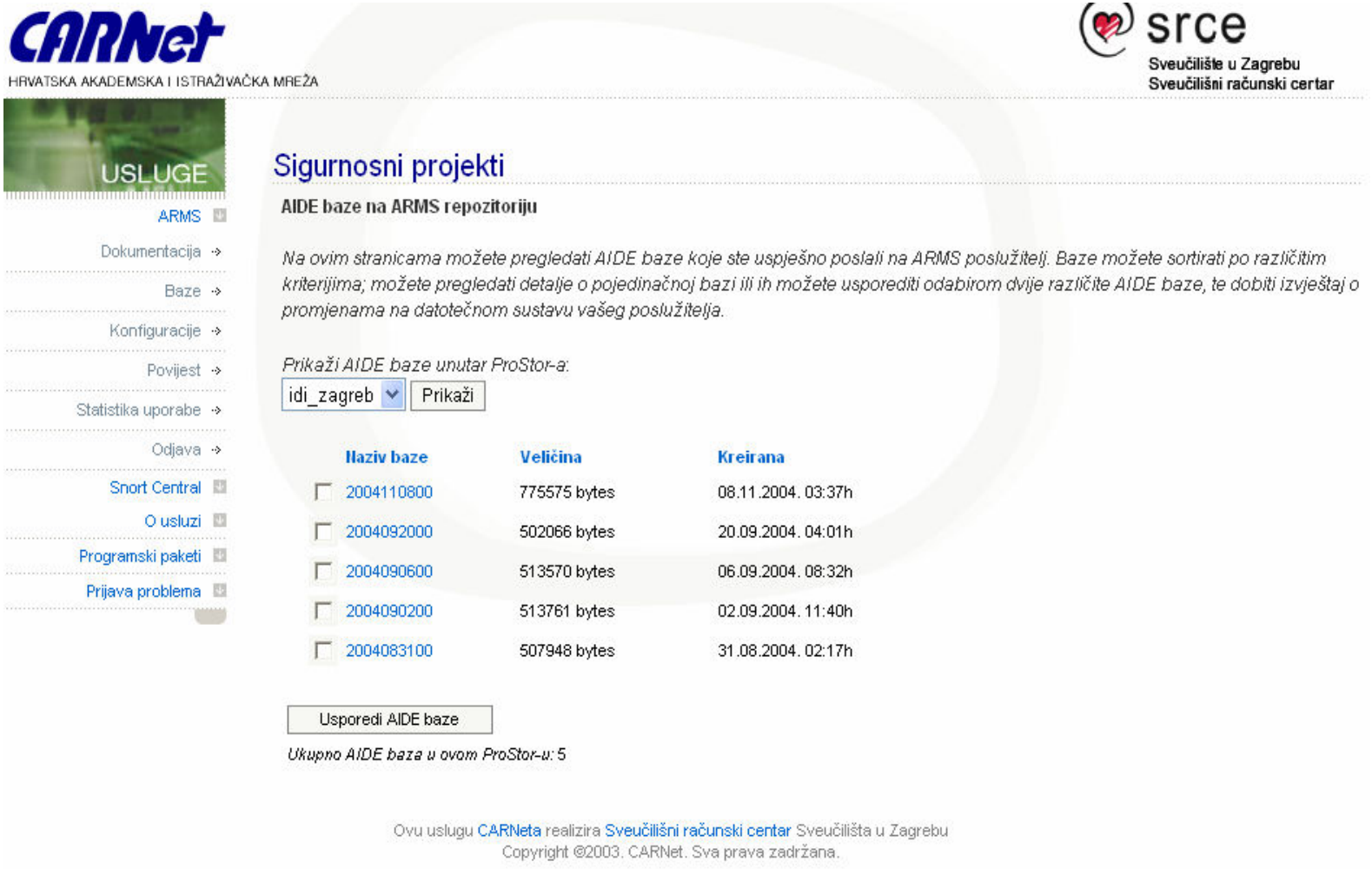
Grafičko sučelje:

Na centralnom poslužitelju:

https://phobos.carnet.hr

- Pristup preko korisničkog imena i zaporke lokalnog LDAP imenika
- Samo za korisnike“A" i “B" skupine
  - A - CARNet ustanove (osoblje, suradnici)
  - B - VIP, CARNet koordinatori, sistem-inženjeri, CMU-administratori

Grafičko sučelje:



Grafičko sučelje:

CARNet
HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA

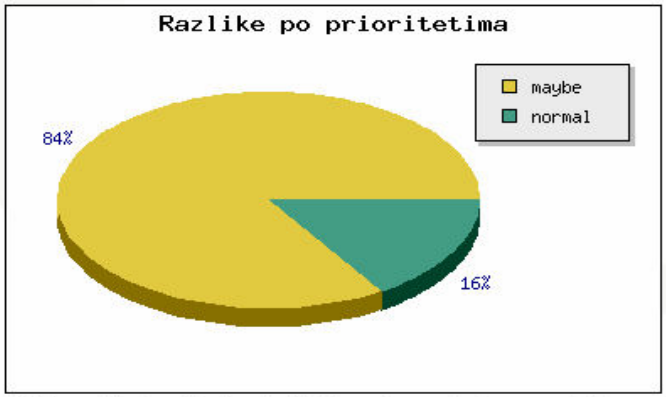
srce
Sveučilište u Zagrebu
Sveučilišni računski certar

USLUGE

- ARMS
- Dokumentacija
- Baze
- Konfiguracije
- Povijest
- Statistika uporabe
- Odjava
- Snort Central
- O usluzi
- Programski paketi
- Prijava problema

Sigurnosni projekti

Analiza razlika između AIDE baza



Kritične razlike, između referente AIDE baze i one sa kojom uspoređujete, označene su bojama radi lakšeg snalaženja u ispisu razlika.

Legenda:

*Kritične razlike - **crvena boja***
*Upitan stupanj kritičnosti - **žuta boja***
*Vjerojatno nebitne razlike - **zelena boja***

/bin

Polje	***Referentna vrijednost***	***Nova vrijednost***
mTime	2004-09-04 10:50:20	2004-08-26 15:05:39
cTime	2004-09-04 10:50:20	2004-08-26 15:05:39

Stari podaci

- Zasad se čuvaju svi podaci
- Kad ponestane prostora, stari podaci će se uklanjati
  - Sistemac će sam birati što ukloniti
  - Ako to ne učini, sustav će automatski oslobađati prostor

Linkovi:

- ARMS:

  https://phobos.carnet.hr

- AIDE:

  http://www.cs.tut.fi/~rammer/aide.html

  http://sourceforge.net/projects/aide

- CARNetovi paketi (sources.list)

  deb http://ftp.carnet.hr/pub/debian/ carnet-sarge main

II Dio: Snort Central

Opis sustava

Instalacija i konfiguracija

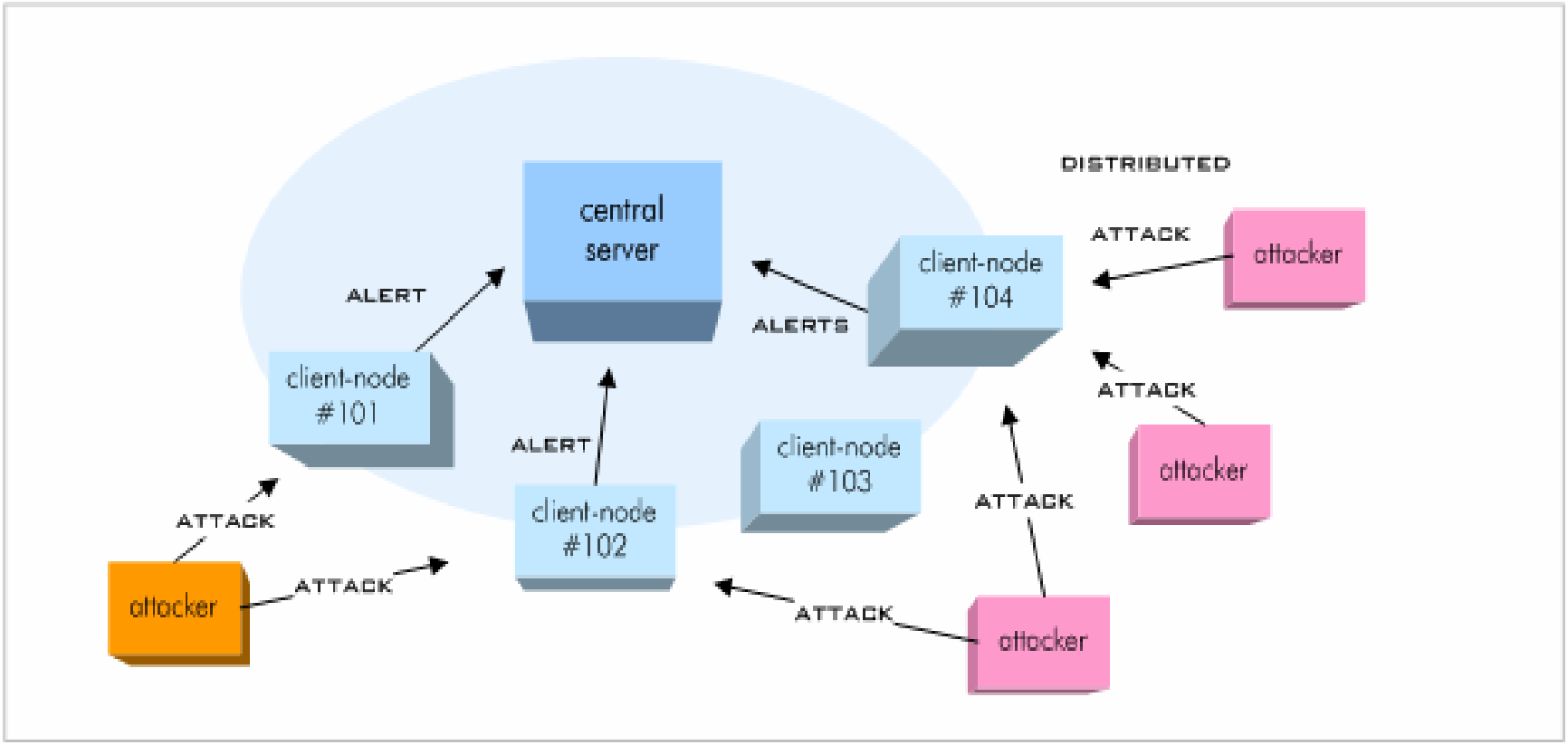
Korištenje

Što je SNORT-Central?

- Sustav za otkrivanje upada u mreži CARNet
- Baziran na open-source rješenju kojeg čine
  - Snort – kao IDS senzor
  - Prelude – baza za obradu podataka dobivenih od senzora, raspoređenih u mreži

Pregled:

Snort Central – centralized network security overview



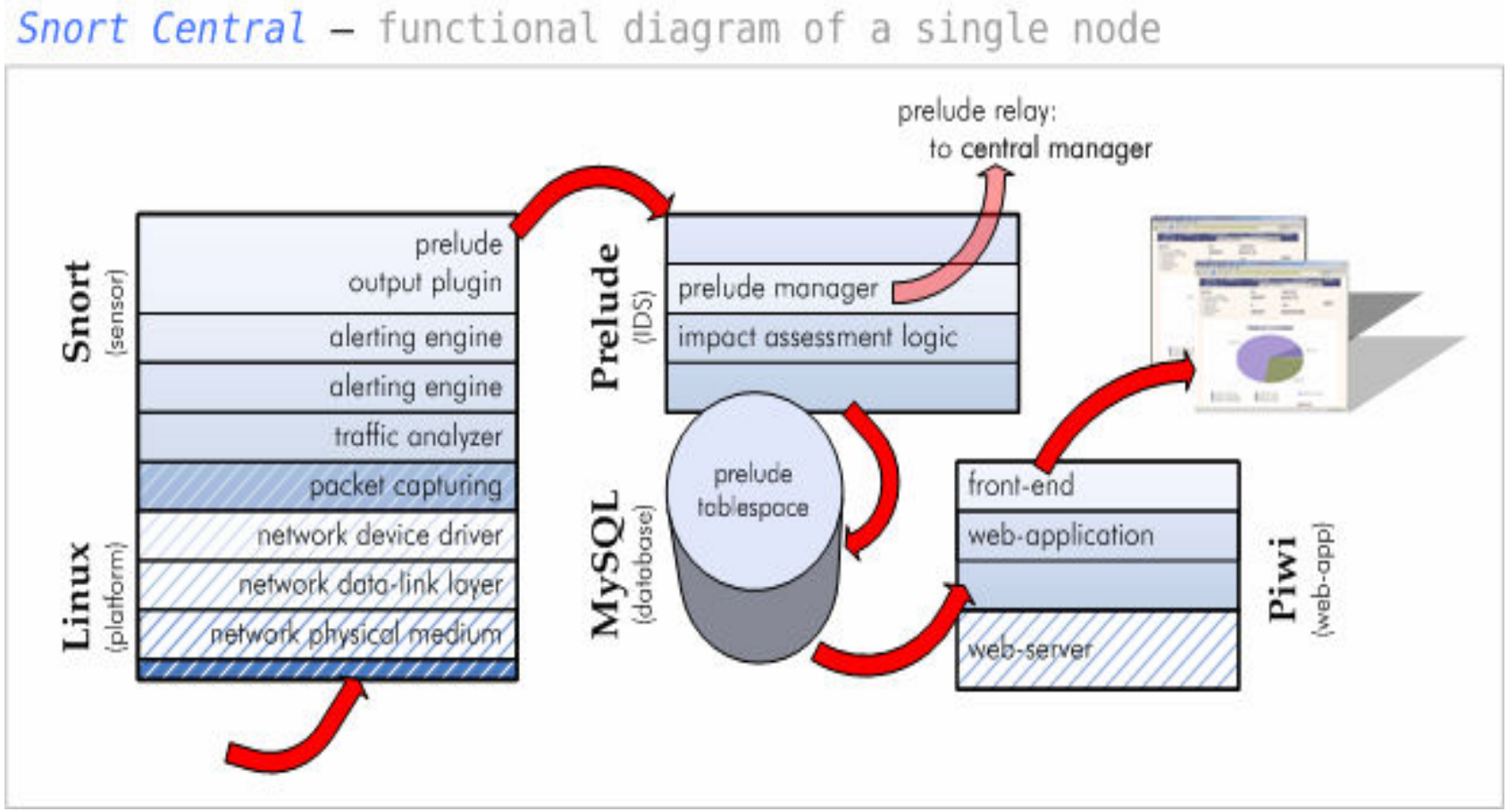
Lokalno ili u CARNetu?

- Dva načina korištenja:
  - Lokalno
    - Lokalni Prelude, jedan ili više senzora u LAN-u
  - U mreži CARNet
    - Ukoliko se uključite u zajednički sustav nadzora
    - Promjena u konfiguraciji, slanje alerta na centralni sustav na Srcu
    - Pregled zbivanja u cijeloj mreži CARNet

Zašto centralni sustav:

- Sustav pod stalnim nadzorom
- Pravovremena reakcija:
  - Upozorenje nadležnom administratoru
  - Konkretna akcija/re-akcija na razini mrežne infrastrukture

Funkcionalni pregled rješenja:



Planiranje!

- Diskovni prostor?
- Procesorska moć?
- Memorija?

- Koliko senzora u mreži?

Diskovni prostor

- Na prosječnom poslužitelju otprilike 100 MB podataka tjedno

- Količina može znatno varirati:
  - U slučaju masovnog napada
  - Ovisi o konfiguraciji

Načini logiranja:

- Tri načina logiranja:
  - ASCII short
    - Kratko, brzo, efikasno, preporučeno
    - SID
    - http://www.snort.org/snort-db/sid.html
  - ASCII long
    - zauzima resurse
    - redundantnost
  - Binary
    - forenzike

Filteri

- Bitno je podesiti pravila da tako da odgovaraju specifičnom sistemu
- Tražiti samo napade na aktivne servise
- Zanemariti napade na nepostojeće servise i aplikacije

Koliko senzora?

- Svaki važan poslužitelj – vlastiti senzor
  - Reagira samo na napade koji se tiču njegovih servisa i aplikacija
  - Svaki VLAN sa vlastitim mrežnim IDS-om
  - Jedan zajednički mrežni IDS za cijelu vašu mrežu
  - Ne morate odmah odlučiti, lako je kasnije dodavati senzore

Procesorska moć

- Ne preporuča se instalacija na mrežne poslužitelje opterećene:
  - velikim mrežnim prometom
  - procesorskim zahtjevima
  - s premalo diskovnog prostora

Alternativa:

- Instaliranje sustava na paralelno nadzorno računalo
- Uporaba specijaliziranog hardvera
  - Repeater
  - Spaning port na switchu

Sastavni dijelovi

- paketi:
  - libprelude0 (dojava)
  - prelude-manager (analiza)
  - snort (detekcija)
  - mysql (...) (podaci)
  - piwi (prikaz)

Te njihove prilagođene "-cn" inačice:

- snort-cn
- snort-central-cn
- prelude-manager-cn
- prelude-sensors-cn
- piwi-cn

Snort-cn:

- Baza karakterističnih uzoraka napada
  - *attack pattern snort rules*
- Distribuira se u paketu *snort-cn*, kojeg je potrebno redovito osvježavati

- Izvor:
  - http://www.snort.org/dl/rules/
  - http://oinkmaster.sourceforge.net/

Snort Central
Instalacija i konfiguracija

Instalacija:

- Kratke upute za instalaciju sustava:

  # apt-get install snort-central-cn

- radi ovisnosti među paketima instalirati će sve potrebno

Instalacija:

```
testhost# apt-get install snort-central-cn
Reading Package Lists... Done
Building Dependency Tree... Done
The following extra packages will be installed:
libprelude0 piwi piwi-cn prelude-manager prelude-manager-cn
prelude-sensors-cn snort-cn snort-common snort-prelude
snort-rules-default
Suggested packages:
snort-doc
Recommended packages:
oinkmaster
The following NEW packages will be installed:
libprelude0 piwi piwi-cn prelude-manager prelude-manager-cn
prelude-sensors-cn snort-central-cn snort-cn snort-common
snort-prelude snort-rules-default
0 upgraded, 11 newly installed, 0 to remove and 70 not
upgraded.
Need to get 404kB/1139kB of archives.
After unpacking 4581kB of additional disk space will be
used.
Do you want to continue? [Y/n] Y
```

Instalacija:

- **apt-get** naredbe će putem definiranih ovisnosti (dependency) instalirati pakete:
  - *libprelude0, prelude-manger, snort-prelude, mysql-server, libmysqlclient10*
  - *libdbd-mysql-perl*
- Slijedi instalacija paketa koji vrše prilagodbu tih radnih komponenti Snort Central sustavu

Instalacija (prelude-manager-db-create-cn.sh):

- Najprije prelude-manager-cn.
  - ukoliko ustanovi da je to prva instalacija pokreće skriptu ”čarobnjaka”

- **prelude-manager-db-create-cn.sh**

Instalacija (prelude-manager-db-create-cn.sh):

- Podešavanje radne okoline Prelude managera:

```
CN: Prelude manager ready to be set up a'la CARNet
CN: ==> use: /usr/sbin/prelude-manager-db-create-cn.sh

Do you want to do it now? (y)es/(n)o: y

Prelude Database Installation
=============================

*** Phase 0/3 ***
Warning: if you want to use database support with prelude
You should dedicate the database for this job only.

Do you want to install a dedicated database for prelude ?
(y)es / (n)o : y
```

Instalacija (prelude-manager-db-create-cn.sh):

- *** Phase 1/3 ***
  This installation script has to connect to your mysql database
  in order to create a user dedicated to stock prelude's alerts

  What is the database administrative user ? [root]: [Enter]

- *** Phase 2/3 *** We need the password of the admin user "root" to log on the database.

  By default under mysql, root has an empty password.

  Please enter a password: [Enter]

  Please confirm entered password: [Enter]

Instalacija (prelude-manager-db-create-cn.sh):

- *** Phase 3/3 ***

  Please confirm those information before processing :

  Database name : prelude
  Database admin user : root
  Database admin password : (not shown)

  prelude owner user : prelude
  prelude owner password : LoiuIELZ

  Is everything okay ? (yes/no) : yes

Instalacija (prelude-manager-db-create-cn.sh):

```
Creating the database prelude...

Creating user "prelude" for database "prelude",
using "root" to connect to the database.

Creating tables with
/usr/share/prelude-manager/mysql/mysql.sql

Prelude database installation completed.

CN: Prelude manager database configured
CN: (Re)start prelude-manager?

Do you want to do it now? (y)es/(n)o: yes

Restarting Prelude Manager: prelude-manager.
```

Instalacija (prelude-sensors-configure.sh):

- Instalacija klijentskog dijela:
  - olakšana paketom prelude-sensors-cn
  - slijedi podešavanja paketa prelude-manager-cn

- U sklopu instalacije pokreće se skripta:
  prelude-sensors-configure.sh

Instalacija (prelude-sensors-configure.sh):

- Prikaz konfiguriranja senzora skriptom prelude-sensors-configure.sh:

```
Setting up prelude-sensors-cn (0.03-1) ...
CN: Generating prelude-manager host key ...
CN: done.

CN: Prelude sensors ready to be set up a'la CARNet
CN: ==> use: /usr/sbin/prelude-sensors-configure.sh

Do you want to do it now? (y)es/(n)o: y

Prelude Sensors Installation Support
====================================
```

- `*** Phase 0/5 ***`

```
Do you want to configure sensors for snort and prelude-manager ?
(y)es / (n)o : yes
```

Instalacija (prelude-sensors-configure.sh):

- *** Phase 1/5 ***

  Enter the DNS name of this node (enter to confirm:\
  testhost.srce.hr):

- *** Phase 2/5 ***

  Enter the location of this node: Test Node

- *** Phase 3/5 ***

  Enter IP address of this node (enter to confirm:\
  192.168.2.22): [Enter]

Instalacija (prelude-sensors-configure.sh):

- *** Phase 4/5 ***

```
Enter IP netmask of this node (in regard to address)
(enter to confirm: 255.255.255.255): [Enter]
```

- *** Phase 5/5 ***

```
Please confirm those information before processing :

Node name: testhost.srce.hr
Node location: Test Node
Node address/netmask: 192.168.2.22/255.255.255.255


Is everything okay ? (yes/no):
Is everything okay ? (yes/no): yes
```

Instalacija (prelude-sensors-configure.sh) :

- Created new /etc/prelude-sensors/sensors-default.conf --- contents:

```
>> # prelude-sensors/sensors-default.conf file
>> # automatically generated by /usr/sbin/prelude-sensors-
configure.sh
>>
>> manager-addr = 127.0.0.1;
>> node-name = testhost.srce.hr;
>> node-location = Test Node;
>> node-category = dns;
>>
>> address = 192.168.2.22;
>> netmask = 255.255.255.255;
>>
>> category = ipv4-addr;
```

- Now you can run prelude-sensors-register.sh to register sensors with manager(s)

Instalacija (**prelude-sensors-register.sh**) :

- Postupak registracije senzora podijeljen je u tri faze:
  1. prijava na lokalni manager-adduser za lokalni senzor: snort
  2. dohvat tajne riječi potrebne za registraciju senzora na udaljeni manager-adduser
  3. prijava na udaljeni manager-adduser na načunalu phobos.carnet.hr, za relay senzor[1]: "prelude-manager“

- Vodi ga skripta: **prelude-sensors-register.sh**

Instalacija (prelude-sensors-register.sh):

```
Now you can run prelude-sensors-register.sh to register sensors with
   manager(s)

   Do you want to do it now? (y)es/(n)o: y

*** Phase 1/3 ***

   Do you want to register snort sensor with local prelude-manager?
   (y)es / (n)o : y

   Starting manager-adduser in background...

   CN: When it starts, copy it's generated password into clipboard
   CN: You'll need it to register sensor with local prelude-manager.
   CN: You may choose any password you want for it, for it will be
   CN: stored in a file on local filesystem and used only locally.

   grep: /etc/prelude-manager/manager.auth: No such file or directory
   Generated one-shot password is >>> ic5020ey <<< [Copy]
```

Instalacija (prelude-sensors-register.sh)

```
Now please start "manager-adduser" on the Manager host
where
you wish to add the new user.

Please remember that you should call "sensor-adduser" for
each configured Manager entry.

Press enter when done.


Please use the one-shot password provided by the
"manager-adduser" program.

Enter registration one shot password : [Paste]
Please confirm one shot password : [Paste]
connecting to Manager host (127.0.0.1:5553)... Succeeded.
```

Instalacija (prelude-sensors-register.sh)

```
Username to use to authenticate : snort

Please enter a password for this user : [Paste]
Please re-enter the password (comfirm) : [Paste]
Register user "snort" ? [y/n] : y
Plaintext account creation succeed with Prelude Manager.
Allocated ident for snort@testhost: 533332225118697965.


Was it successfull or should we repeat? (s)uccess /
(r)epeat: s
```

Instalacija (prelude-central-getpass.pl)

- Spajanje na centralni Prelude manager
- Dostupno CARNetovim korisnicima iz skupina A i B

```
*** Phase 2/3 *** Do we need to fetch remote manager-adduser
password? (y)es / (n)o : y

********** /usr/sbin/prelude-central-getpass.pl ***********
```

Instalacija (prelude-central-getpass.pl)

```
****************** /usr/sbin/prelude-central-getpass.pl ******************

This utility script will contact central server to provide you
with password needed to authenticate while registering prelude
sensors using sensor-adduser.

For that purpose you'll need to authenticate to the remote server
using your CARNet CMU/LDAP credentials to remote server.

Communication with server is secured using SSL, and your password
won't be echoed on screen.

Enter your CARNet CMU/LDAP username: test.srce
Enter your CARNet CMU/LDAP password: [ne vidi se]
Contacting server... done.

Today's remote manager-adduser's password is >>> rEP26hcD <<< [Copy]
Copy it in your clipboard for easier use.

****************** /usr/sbin/prelude-central-getpass.pl ******************
```

Instalacija (prelude-central-getpass.pl):

- Registriranje relay senzora "prelude-manager":

```
*** Phase 3/3 *** Do you want to register "prelude-manager"
sensor with remote prelude-manager?
(y)es / (n)o : y

CN: You'll need to provide password-of-the-day from central
server

Now please start "manager-adduser" on the Manager host where
you wish to add the new user.

Please remember that you should call "sensor-adduser" for each
configured Manager entry.

Press enter when done.
```

Instalacija (prelude-central-getpass.pl):

```
Please use the one-shot password provided by the "manager-
adduser" program.

Enter registration one shot password : [Paste]
Please confirm one shot password : [Paste]
connecting to Manager host (phobos.carnet.hr:5553)...
Succeeded.

What keysize do you want [1024] ? [Enter]

Please specify how long the key should be valid.
0 = key does not expire
<n> = key expires in n days

Key is valid for [0] : [Enter]


Key length : 1024
Expire : Never
```

Instalacija (prelude-central-getpass.pl):

```
Is this okay [yes/no] : yes
Generating a 1024 bit RSA private key...
..........++++++
..............++++++

Writing new private key to
'/etc/prelude-sensors/ssl/prelude-manager-key.0'.

Adding self signed Certificate to
'/etc/prelude-sensors/ssl/prelude-manager-key.0'

writing Prelude Manager certificate.

Allocated ident for prelude-manager@testhost:
59538583530191O773.

Was it successfull or should we repeat? (s)uccess / (r)epeat: s
```

Instalacija (snort-central-cn):

- Paket snort-central-cn je noseća komponenta instalacije ovog sustava.
- Automatska konfiguracija adrese sučelja na kojoj Snort prati promet (eth0 adresa host računala)

```
Setting up snort-central-cn (2.2.0-3) ...

CN: Configuring snort to listen only for 192.168.2.22/32 on
   eth0 interface
```

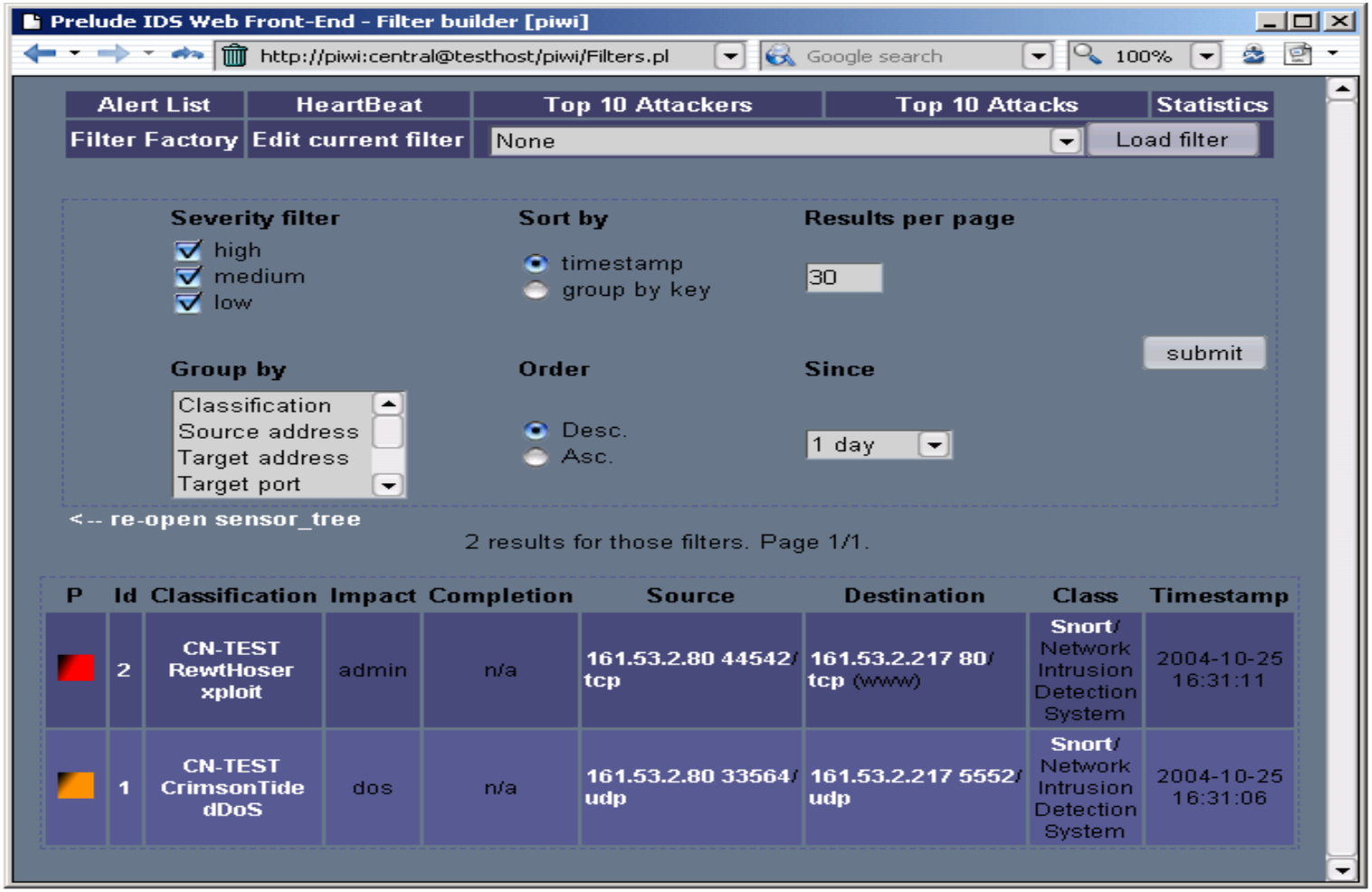
Piwi

- IDS web interface
- http://packages.debian.org/unstable/admin/piwi
- Omogućuje pregled baze podataka Prelude managera koja sadrži prikupljene zapise o uočenom mrežnom prometu.
- piwi-cn - konfiguracijske prilagodbe

Piwi-cn

- CARNetov paket dodaje mogućnost:
  - zaštite web-sučelja korisničkim imenom i lozinkom (basic authorization)
  - uključenje mod_perl modula Apache web servera

Web-sučelje:


Prelude IDS Web Front-End - Filter builder [piwi]
http://piwi:central@testhost/piwi/Filters.pl
Google search
100%
Alert List
HeartBeat
Top 10 Attackers
Top 10 Attacks
Statistics
Filter Factory
Edit current filter
None
Load filter
Severity filter
high
medium
low
Sort by
timestamp
group by key
Results per page
30
submit
Group by
Classification
Source address
Target address
Target port
Order
Desc.
Asc.
Since
1 day
<-- re-open sensor_tree
2 results for those filters. Page 1/1.
P
Id
Classification
Impact
Completion
Source
Destination
Class
Timestamp
2
CN-TEST RewtHoser xploit
admin
n/a
161.53.2.80 44542/ tcp
161.53.2.217 80/ tcp (www)
Snort/ Network Intrusion Detection System
2004-10-25 16:31:11
1
CN-TEST CrimsonTide dDoS
dos
n/a
161.53.2.80 33564/ udp
161.53.2.217 5552/ udp
Snort/ Network Intrusion Detection System
2004-10-25 16:31:06

Dodatne skripte:

- (wrapper) skripta:
  /usr/sbin/prelude-db-cleanup.sh

- Čisti bazu od zastarjelih ili suvišnih podataka

Ručno pokretanje

- **/etc/init.d/snort-central restart**
- ispravnim redoslijedom pokreće prelude-manager i snort

Snort pravila:

- Jednostavni logički uvijeti za detektiranje napada
- Ispituju zaglavlja ili payload paketa

- Dokumentacija:
  - http://www.snort.org/docs/writing_rules/
  - http://www.snort.org/docs/snort_manual/

Snort pravila:

- Alert mode:
  - -A <mode> full,fast,none,console
  - -s syslog
  - -M <wrkstn> SMB winpopup
- Logging mode
  - -b binarni
  - -N no logs

Snort (ASCII log)

FULL:

```
[**] [1:615:3] SCAN SOCKS Proxy attempt [**]
[Classification: Attempted Information Leak] [Priority: 2]
01/24-10:08:48.286291 24.83.20.27:10611 -> 161.53.2.74:1080
TCP TTL:214 TOS:0x0 ID:0 IpLen:20 DgmLen:52 DF
******S* Seq: 0x5CDBD68D  Ack: 0x0  Win: 0xA7A1  TcpLen: 32
TCP Options (5) => MSS: 1460 NOP NOP SackOK NOP
[Xref => http://help.undernet.org/proxyscan/]
```

FAST:

```
01/28-12:21:55.896858  [**] [1:469:3] ICMP PING NMAP [**] [Classification:
Attempted Information Leak] [Priority: 2] {ICMP} 161.53.2.80 -> 161.53.156.3

01/28-12:21:56.052941  [**] [1:1421:11] SNMP AgentX/tcp request [**]
[Classification: Attempted Information Leak] [Priority: 2] {TCP}
161.53.2.80:52395 -> 161.53.156.3:705

01/28-12:21:56.563780  [**] [1:1420:11] SNMP trap tcp [**] [Classification:
Attempted Information Leak][Priority: 2] {TCP} 161.53.2.80:52395 ->
161.53.156.3:162
```

Snort log (tekstualni):

- ASCII format
- Čitko
- -h “home net”
- Log u direktorije koji se zovu po IP adresi
- Brzo vidimo tko “kuca na vrata”

Snort NIDS:

- Najčešći i najkompleksniji način rada
- Učita skup pravila i dodataka za analizu paketa
- Podrazumjevana konfiguracija u:
  - /etc/snort.conf
- Logdir:
  - Unix: /var/log/snort
- Alert mode: full
- Log: ASCII

Poruka razvojnog tima:

- Objavljeni projekti prošli su osnovno testiranje,
- Željeli simo čuti vašu povratnu informaciju, kao i sugestije za poboljšanja

- Prijedloge, bugove, ideje, zahtjeve za pomoć... uputite helpdesku za sistem-inženjere:

  sistemac@carnet.hr
  http://sistemac.carnet.hr/syshelp

Upute za daljnje čitanje

- phobos.carnet.hr
- www.snort.org
- Seminari:
  - IDS ...

    http://sistemac.carnet.hr/fileadmin/sem/IDS/Otkrivanje_upada.pdf
  - Implementacija sigurnosne politike

    http://sistemac.carnet.hr/fileadmin/sem/SigPol/ImplementacijaPolitike.pdf

I na kraju...

- Preporučujemo Vam korištenje IDS servisa kako bismo popravili sigurnost
  - Vašeg LAN-a
  - Mreže CARNet
- Prilika za učenje!